AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One VHS video cassette, one SmartDisk Firelite external hard drive, one black external hard drive (unknown make and model), and one Corsair Flash Voyager thumb drive

Case No. 2:13mj582

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT B

located in the SOUTHERN District of OHIO, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 2252	Receipt, distribution, and/or possession of visual depictions of minors engaged in sexually explicit activity and/or child pornography, via a means or facility of interstate commerce.
18 U.S.C. Section 2252A	

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brett M. Peachy, FBI TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/31/13

Judge's signature

City and state: Columbus, OH

Honorable Terrence P. Kemp, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.**
	)	
One VHS video cassette, one SmartDisk Firelite	)	
external hard drive, one black external hard drive	)	
(unknown make and model), and one Corsair Flash	)	
Voyager thumb drive.	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Violent Crimes Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including the online exploitation of children.

2. During my career as a police and task force officer, I have participated in various investigations of computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitations and child pornography including violations pertaining to the illegal distribution, transmission, receipt, and

possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other subjects and witnesses. I have not included in this affidavit all information known by me relating to the investigation. I have only set forth facts to establish probable cause for a search warrant of one VHS videocassette, one SmartDisk Firelite external hard drive, one black external hard drive (unknown make and model), and one Corsair Flash Voyager thumb drive (the LISTED ITEMS). The LISTED ITEMS were retrieved with consent from the resident located at 6886 Blue Church Road, Sunbury, OH 43074. I have not withheld any evidence or information that would negate probable cause.

5. The LISTED ITEMS to be searched are more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A – the distribution, transmission, receipt, or possession of child pornography.

III. APPLICABLE STATUTES

6. Title 18 United States Code § 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct. For purposes of this statute, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) "

A. as "actual or simulated–

i. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

ii. bestiality;

iii. masturbation;

iv. sadistic or masochistic abuse; or

v. lascivious exhibition of the genitals or pubic area of any person."

7. Title 18 United States Code § 2252A makes it a crime to knowingly mail, transport, ship,

receive, distribute, reproduce for distribution, sell or possess child pornography in interstate commerce. It also makes it a crime to advertise, distribute or solicit in interstate commerce any material that reflects the belief or is intended to cause another to believe that the material contains an obscene visual depiction of a minor engaging in sexually explicit conduct or a visual depiction of an actual minor engaging in sexually explicit conduct. For purposes of this statute, the term "child pornography" is defined in 18 U.S.C. § 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

B. such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

C. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." The term "sexually explicit conduct" has the same meaning as in 18 U.S.C. § 2252, except for the section (B) definition of child pornography where it means:

i. graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

ii. graphic or lascivious simulated; (I) bestiality; (II) masturbation; (III) sadistic or masochistic abuse; or

iii. graphic or simulated lascivious exhibition of the genitals or pubic area of any person."

8. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. 18 U.S.C. § 2256(10).

9. The following terms have the same meanings or explanations in both statutes:

A. "minor" means any person under the age of eighteen years, pursuant to 18 U.S.C. § 2256(1);

B. "visual depiction" includes undeveloped film and videotape, and data stored on

computer disk or by electronic means which is capable of conversion into a visual image, pursuant to 18 U.S.C. § 2256(5);

C. "computer" is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING COMPUTERS AND DIGITAL STORAGE DEVICES

10. I know from my training and experience that computer hardware, software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of the crime in the form of electronic data. Rule 41 of the federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, instrumentalities of crime and/or fruits of crime.

11. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard-drive and can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the files does not actually disappear; rather the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is space on the hard drive that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

12. Computers are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

13. Computers are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

14. A computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 100 gigabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine

all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

16. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

17. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §2252, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

18. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to

determine whether that data falls within the list of items to be seized as set forth herein;

c. surveying various files, directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

19. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily- available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

VII. INVESTIGATION AND PROBABLE CAUSE`

20. On October 30, 2013, your affiant was advised of a complaint filed through the FBI by Julie Bowen-Miller alleging that she had discovered various pieces of digital media depicting files of child pornography within her residence at 6886 Blue Church Road Sunbury, OH 43074

21. On the above date, TFO Peachey travelled to Julie Miller's residence where she was

interviewed about the complaint.

22. Julie Miller (herein referred to as Julie) advised that, approximately two years ago, she was utilizing a laptop computer that she shared with her husband, Stewart A. MILLER (herein referred to as MILLER). While using the computer, Julie observed approximately twenty five images depicting nude underage females saved to the computer's hard drive. When Julie asked MILLER about the images, he surmised that they had been downloaded by Julie's then teenage son.

23. In July of 2013, Julie observed a thumb drive located in MILLER's bedroom. According to Julie, she and MILLER sleep in separate rooms for personal reasons. Believing that the thumb drive contained photos from a recent family vacation, Julie accessed the photos and observed several folders which contained dozens of images depicting underage and prepubescent females in various forms of undress and nudity, including the lascivious display of their genitals. When Julie confronted MILLER about the images on the drive, she advised that he "downplayed" it and advised that it was just a curiosity and that he would not view or save photos like that in the future. Several days later, Julie searched for the thumb drive again in MILLER's room but could not locate it.

24. Due to what she had observed on the computer and thumb drive, Julie searched various areas of the residence during the months of July and August 2013. Julie first searched MILLER's bedroom and observed a VHS tape located in a VCR. Julie watched portions of the videotape and noticed that the video was of the family's upstairs living room. It occurred to Julie that it appeared as if there was a video camera located within the room that had been recording the room. From the angle of the video, Julie was able to search the living room and locate a small camera hidden beneath an entertainment center.

25. Julie continued to search the residence for anything unusual and searched a crawl space located in the ceiling of MILLER's bathroom. Located in the crawl space was a VHS tape, a SmartDisk Firelite external hard drive, an unknown model external hard drive, and a Corsair Flash Voyager thumb drive.

26. Julie viewed a short amount of the VHS tape, which depicted the same scene of the family's upstairs living room that Julie had seen on the first VHS tape. The recording on the VHS tape Julie found in the crawl space depicted her then seventeen-year-old son engaging in sexual activity with his then seventeen-year-old girlfriend. According to Julie, she became very upset after watching the video and destroyed the video cassette.

27. Approximately three days prior to the interview (on or about October 27, 2013), Julie viewed the contents of the Flash Voyager thumb drive and SmartDisk Firelite external hard drive that she had also retrieved from the crawl space. According to Julie, both drives contained images and videos of underage and prepubescent females in various stages of dress and nudity including the lascivious display of their genitals. Julie specifically recalls one video depicting a prepubescent female, approximately eight to ten years of age, masturbating.

28. Julie voluntarily turned over the above listed VHS tape, two external drives, and thumb drive to your affiant, along with a signed consent to search form. Julie informed your affiant that MILLER was currently out of town, but was due back within the next few days. The items Julie turned over were therefore taken for safekeeping, and are currently located at the FBI Columbus Resident Agency 425 W. Nationwide Blvd, Columbus, OH 43215. Neither your affiant nor any other law enforcement officer has searched any of these items since they were turned over by Julie.

VIII. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

29. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

A. Those who receive and may be collecting child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

B. Those who receive and may be collecting child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who receive and may be collecting child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist – that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

D. Likewise, those who receive and may be collecting child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

E. Those who receive and may be collecting child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

F. Those who receive and may be collecting child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

G. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

30. Based upon the conduct of individuals involved in the collection of child pornography set forth in the above paragraph, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media,

there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located on the LISTED ITEMS

IX. CONCLUSION

31. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and 2252A have been committed, and evidence of those violations is located in the LISTED ITEMS described in Attachment B. Your affiant respectively requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

32. Your affiant asserts that public disclosure of the existence of this search warrant affidavit and all accompanying materials at this juncture could jeopardize the government's ongoing investigation in this case and therefore requests this affidavit and all accompanying material be sealed until further order of the this Court.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 31st day of October 2013.

Honorable Terrence P. Kemp
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A

LIST OF ITEMS TO BE SEIZED

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages) pertaining to the possession, receipt, or distribution of child pornography, or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography, visual depictions, or child erotica.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography or any visual depictions.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals

about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
14. Any and all visual depictions of minors.
15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.
16. Any and all digital diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED

1. One unmarked VHS video cassette;
2. One Smart Disk Firelite external hard drive;
3. One black external hard drive (unknown make and model); and
4. One Corsair FlashVoyager thumb drive.

All of the above items were located by the resident 6886 Blue Church Road Sunbury, OH 43074, within a crawl space of her residence and were voluntarily turned over to law enforcement.